

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS**

Leaha Sweet, on behalf of herself and all others similarly situated,

Plaintiff,

v.

BJC Heath System d/b/a BJC Healthcare,

Defendant.

Case No.:

CLASS ACTION COMPLAINT

COMES NOW Leaha Sweet, individually and on behalf of all others similarly situated, by and through her attorneys, and files this Class Action Petition against Defendant BJC Heath System d/b/a BJC Healthcare and alleges as follows:

PARTIES

1. Plaintiff, individually and as class representative, is a resident of Madison County, Illinois.
2. Defendant BJC Heath System d/b/a BJC Healthcare is a Missouri nonprofit corporation that maintains its principal place of business in Missouri.
3. The Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) in that this is a class action in which the matter in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, and in which any member of the class of plaintiffs is a citizen of a state different from any defendant.
4. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1331(b)(2), as a

substantial part of the events or omissions giving rise to the claim occurred in this district.

INTRODUCTION

5. This is a consumer class action lawsuit brought by Plaintiff, individually and on behalf of all similarly situated persons who are citizens of Illinois (“Class Members”), whose personally identifiable information and personal health information (e.g., name, address, birthdate, telephone number, and social security numbers, and, possibly including credit card, medical, or clinical information) (“PHI”)—which is considered protected under the Health Insurance Portability and Accountability Act (“HIPAA”)—was entrusted to Defendant and was stolen, disclosed, and/or made accessible to hackers and identity thieves.

6. As a result of Defendant’s failure to implement and follow basic security procedures, the PHI of patients (including Plaintiff and Class Members) was made accessible to thieves.

7. Plaintiff and Class Members now face a substantially increased risk of additional instances of identity theft and resulting losses.

8. Plaintiff and Class Members are immediately and imminently in danger of sustaining some or further direct injury/injuries as a result of the identity theft they suffered when Defendant did not protect and secure the PHI and disclosed the PHI to hackers. These further instances of identity theft are impending and imminent. The PHI has all the information wrongdoers need, and the American government and financial system require, to completely and absolutely misuse Plaintiff’s and Class Members’ identity to their detriment.

9. Consequently, Defendant’s customers and former customers have or will have to spend significant time and money to protect themselves, including, but not limited to: the cost of responding to the data breach, cost of conducting a damage assessment, mitigation costs, costs to

rehabilitate Plaintiff's and Class Members' PHI, and costs to reimburse from losses incurred as a proximate result of the breach.

10. Additionally, as a result of Defendant's failure to follow contractually-agreed upon, federally-prescribed, industry-standard security procedures, Plaintiff and Class Members received a diminished value of the services they paid Defendants to provide.

FACTS COMMON TO ALL COUNTS

11. Plaintiff and Class Members are customers of Defendant and provided payment to Defendant for certain services, part of which was intended to pay the administrative costs of securing their respective PHI.

12. Plaintiff and Class Members contracted for services that included a promise by Defendant to safeguard, protect, and not disclose their personal information and, instead, Plaintiff and Class Members received services devoid of these vital protections.

13. On March 6, 2020, an unauthorized person gained access to the employee email accounts of three of Defendant's employees. One or more emails and/or attachments to which this person gained access included Plaintiff's and each Class Member's name, date of birth, medical record or patient account number, and/or treatment and/or clinical information, such as diagnosis, medications, provider, type of treatment, and treatment location.

14. As a proximate result of Defendant's wrongful acts and omissions, Plaintiff and the Class Members have suffered injury, harm, and damages, including, but not limited to, loss of monies paid to Defendant for services to protect and not disclose PHI, and Plaintiff and Class Members have and will have to spend significant time and money to protect themselves, including, but not limited to: the cost of responding to the data breach, cost of conducting a damage assessment, costs to obtain credit reports, costs to obtain future credit reports, costs for credit monitoring, costs for insurance to

indemnify against misuse of identity, costs to rehabilitate Plaintiff's and Class Members' PHI, and costs to reimburse from losses incurred as a proximate result of the breach. All of these damages are fairly traceable to Defendant's actions.

HIPAA & HTTECH ACT REQUIREMENTS

15. Under HIPAA and the HITECH Act, Defendant must implement policies and procedures to limit physical access to their electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. *See 45 C.F.R. § 164.310.*

16. Specifically, Defendant must ensure the confidentiality, integrity, and availability of all electronic PHI Defendants, or any entity for, on behalf of, at the request of, in furtherance of the responsibilities or obligations of, or pursuant to a contractual responsibility of Defendant's behalf ("Agents"), creates, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of such information and protect against any reasonably anticipated uses or disclosures of such information that are not permitted. *See 45 C.F.R. § 164.306.*

17. Defendant must also implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights as specified in 45 C.F.R. § 164.308(a)(4). A few of these policies and procedures include, but are not limited to: implementing a mechanism to encrypt and decrypt electronic PHI; implementing hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI; implementing procedures to verify that a person or entity seeking access to electronic PHI is the claimed; implementing technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network; and implementing security

measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of. *See 45 C.F.R. § 164.312.*

18. When Defendant permits Agents to create, receive, maintain, or transmit electronic PHI, Defendant must ensure those Agents comply with HIPAA and the HITECH Act. *See 45 C.F.R. § 164.314.*

19. Defendant must also conduct accurate and thorough assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by Defendant or Agents; implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports; and implement procedures for guarding against, detecting, and reporting malicious software. *See 45 C.F.R. § 164.308.*

20. Defendant did not comply with any of the foregoing requirements.

DEFENDANT DID NOT PROTECT PLAINTIFF'S AND CLASS MEMBERS' PHI

21. Defendant did not comply with, and therefore violated, HIPAA and HITECH Act.

22. Defendant and Agents stored Plaintiff's and Class Members' PHI in an unprotected, unguarded, unsecured, and/or otherwise unreasonably protected electronic and/or physical location.

23. Defendant and Agents did not adequately encrypt, if at all, Plaintiff's and Class Members' PHI.

24. Defendant and Agents did not provide adequate security measures to protect Plaintiff's and Class Members' PHI.

25. On April 8, 2014, the FBI issued a Private Industry Notification to the healthcare industry, warning:

Cyber actors will likely increase cyber intrusions against health care systems - to include medical devices - due to mandatory transition from paper to electronic

health records (EHR), lax cybersecurity standards, and a higher financial payout for medicalrecords in the black market ... the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques, and procedures (TTPs), much less against more advanced persistent threats (APTs). The health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely.

26. The notification continued by detailing the value of Plaintiff's and Class Members' PHI: "Cyber criminals are selling the information on the black market at a rate of \$50 for each partial EHR, compared to \$1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft."

27. Upon information and belief, the data breaches were solely to steal Plaintiff's and Class Members' identity by accessing, transferring, and copying the PHI Defendant electronically stored.

28. The data accessed, copied, and transferred included information protected under HIPAA because it included patient names, addresses, birthdates, telephone numbers, and social security numbers and may have included patient credit card, medical, and/or clinical information.

29. Upon information and belief, Defendant and Agents did not design and implement policies and procedures for the security of electronically stored PHI.

30. If Defendant or Agents did design and implement policies and procedures for the security of electronically stored PHI, these policies and procedures failed to adhere to reasonable and best industry practices in safeguarding PHI.

31. Upon information and belief, Defendant and Agents failed to encrypt, or adequately encrypt, Plaintiff's and Class Members' PHI.

32. By failing to fulfill its promise to protect Plaintiff's and Class Members' PHI, Defendant has deprived Plaintiff and Class Members of the benefit of the bargain. As a result, Defendant cannot equitably retain payment from Plaintiff and Class Members—part of which was intended to pay for the administrative costs of data security—because Defendant did not properly secure Plaintiff's and Class Members' information and data.

CLASS ACTION ALLEGATIONS

33. Class: Plaintiff brings this action on behalf of herself and a statewide class of similarly situated individuals, defined as follows:

All citizens of Illinois who are current or former customers of BJC whose PHI was accessed, copied, or transferred by an unauthorized person on or around March 6, 2020.

34. Excluded from the Class Members are (i) any judge presiding over this action and members of their families; (ii) Defendant, Defendant's subsidiaries, parents successors, predecessors, and any entity in which Defendant or its parents have a controlling interest and its current or former offices and directors; (iii) employees who (a) have or had a managerial responsibility on behalf of the organization, (b) whose act or omission in connection with this matter may be imputed to the organization for purposes of civil liability, or (c) whose statement may constitute an admission on the part of Defendant; (iv) persons who properly execute and file a timely request for exclusion from the class; (v) the attorneys working on Plaintiff's claims; and (vi) the legal representatives, successors, or assigns of any such excluded persons, as well as any individual who contributed to the unauthorized access of the data stored by Defendant.

35. Numerosity. Upon information and belief, the Class Members includes thousands, making their individual joinder herein impracticable. Although the exact number of Class Members and their addresses are unknown to Plaintiff, they are readily ascertainable from Defendant's records.

Class Members may be notified of the pendency of this action by mail and/or electronic mail, and supplemented (if deemed necessary or appropriate by the Court) by published notice.

36. Typicality. Plaintiffs' claims are typical of the Class Members because Plaintiff and the Class Members sustained damages as a result of Defendant's uniform wrongful conduct during transactions with Plaintiff and the Class Members.

37. Adequacy. Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class Members she seeks to represent. Plaintiff has retained competent and experienced counsel, and Plaintiff intends to prosecute this action vigorously. The interest of Class Members will be treated fairly and adequately protected by Plaintiff and her counsel.

38. Predominance and Superiority. This class action is appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy and joinder of all Class Members is impracticable. The damages suffered by the individual Class Members will likely be small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' wrongful conduct. Thus, it would be virtually impossible for the individual Class Members to obtain effective relief from Defendant's misconduct. Even if Class Members could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered, and uniformity of decisions will be ensured.

39. Commonality. Common questions of law and fact exist as to all Class Members and predominate over any questions affecting only individual members, and include, but are not limited

to:

- a. Whether Defendant was negligent in collecting, storing, protecting, and/or securing Plaintiff's and the Class Member's PHI;
 - b. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PHI;
 - c. Whether Defendant breached its duty to exercise reasonable care in handling Plaintiff's and Class Members' PHI by storing that information in the manner alleged herein;
 - d. Whether Defendant disclosed Plaintiff's and Class Members' PHI;
 - e. Whether implied or express contracts existed between Defendant and Plaintiff and Class Members;
 - f. Whether Plaintiff and the Class Members are at an increased risk of identity theft or other malfeasance as a result of Defendant's failure to protect their PHI;
 - g. Whether Defendant stored PHI in a reasonable manner consistent with industry standards;
 - h. Whether protecting Plaintiff's PHI was a service provided by Defendant;
 - i. Whether Defendant has unlawfully retained payment from Plaintiff and Class Members because of Defendant's failure to fulfill its agreement to protect, secure, keep private, and not disclose Plaintiff's and Class Members' PHI; and
 - j. Whether and to what extent Plaintiff and the Class Members have sustained damages.
40. Plaintiff reserves the right to revise Class definitions and questions based upon facts learned in discovery.

COUNT I: UNJUST ENRICHMENT

41. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

42. Defendant received payment from Plaintiff and Class Members to perform services that included protecting, securing, keeping private, and not disclosing Plaintiff's and Class Members' PHI.

43. Defendant agreed to ensure Agents complied with the same obligations as Defendant with respect to the protection of Plaintiff's and Class Members' PHI.

44. Defendant did not protect, secure, and/or keep private Plaintiff's and Class Members' PHI and/or disclosed Plaintiff's and Class Members' PHI, but retained Plaintiff's and Class Members' payments.

45. Defendant has knowledge of said benefit.

46. Defendant has been unjustly enriched, and it would be inequitable for Defendant to retain Plaintiff's and Class Members' payments.

47. As a result, Plaintiff and Class Members have been proximately harmed and/or injured.

COUNT II: BREACH OF CONTRACT (EXPRESS AND/OR IMPLIED)

48. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein, excluding Count I.

49. Plaintiff and Class Members paid money to Defendant in exchange for services, which included promises to secure, safeguard, protect, keep private, and not disclose Plaintiff's and Class Members' PHI.

50. In documents that memorialize the obligations of the parties, Defendant promised

Plaintiff and Class Members that Defendants would protect, secure, keep private, and not disclose Plaintiff's and Class Members' PHI.

51. These documents were provided in a manner and during a time where they became part of the agreement for services.

52. Defendant promised to comply with all HIPAA standards and to ensure Plaintiff's and Class Members' PHI was protected, secured, kept private, and not disclosed.

53. In the alternative, to the extent it was not expressed or, again in the alternative, an implied contract existed in the absence of an express contract whereby, Defendant promised to comply with all HIPAA standards and regulations and to ensure Plaintiff's and Class Members' PHI was secured, safeguarded, kept private, protected, and not disclosed to third parties.

54. To the extent it was not expressed, an implied contract was created whereby Defendant promised to safeguard Plaintiff's and Class Members' health information and PHI from being accessed, copied, and transferred by or disclosed to third parties.

55. In the alternative, an express contract did not exist, but an implied contract existed between the parties whereby, in exchange from monies from Plaintiff and Class Members, Defendant agreed to protect, safeguard, secure, keep private, and not disclose to third-parties Plaintiff's and Class Members' PHI.

56. Under the implied contract, Defendant was also obligated to provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PHI.

57. Defendant agreed to ensure Agents complied with the same obligations as Defendant with respect to the protection of Plaintiff's and Class Members' PHI.

58. Defendants did not secure, safeguard, protect, and/or keep private Plaintiff's and

Class Members' PHI and/or disclosed their PHI to third parties, and therefore Defendant breached its contracts with Plaintiff and Class Members.

59. Defendant allowed third parties to access, copy, and/or transfer Plaintiff's and Class Members' health information and PHI, and therefore Defendant breached its contracts with Plaintiff and Class Members.

60. Furthermore, Defendant's failure to satisfy its confidentiality and privacy obligations resulted in Defendant providing services to Plaintiff and Class Members that were of a diminished value.

61. As a result, Plaintiff and Class Members have been harmed, damaged, and/or injured.

COUNT III: NEGLIGENCE

62. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein, excluding Counts I and II.

63. Defendant requested and came into possession of Plaintiff's and Class Members' PHI and had a duty to exercise reasonable care in securing, safeguarding, keeping private, and protecting such information from being accessed by and disclosed to third parties. Defendant's duty arose from the industry standards discussed above and Defendant's relationship with Plaintiff and Class Members.

64. Defendant had a duty to have procedures in place to detect and prevent improper access and misuse of Plaintiff's and Class Members' PHI. The breach of security, unauthorized access, transfer of data, and resulting injury to Plaintiff and the Class Members were reasonably foreseeable, particularly given Defendant's inadequate data security systems and failure to adequately encrypt the data.

65. Defendant agreed to ensure Agents complied with the same obligations as Defendant with respect to the protection of Plaintiff's and Class Members' PHI.

66. Defendant had duties defined by HIPAA, and Defendant breached those duties.

67. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to implement industry standard protocols and/or exercise reasonable care in protecting, securing, keeping private, safeguarding, and not disclosing Plaintiff's and Class Members' PHI.

68. Defendant, through actions and/or omissions, breached its duty to Plaintiff by failing to have procedures in place to detect and prevent access to Plaintiff's and Class Members' PHI by unauthorized persons.

69. But for Defendant's breach of duties, Plaintiff's and Class Members' PHI would not have been accessed, copied, transferred, and/or disclosed.

70. Plaintiff's and Class Members' PHI was accessed, copied, transferred, and/or disclosed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding, securing, protecting, and keeping private such information by adopting, implementing, and maintaining appropriate security measures and encryption.

71. As a result, Plaintiff and Class Members have been harmed, damaged, and/or injured.

COUNT IV: CONSUMER FRAUD ACT

72. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein, excluding Counts I, II, and III.

73. At all times relevant hereto, the Illinois Consumer Fraud and Deceptive Business

Practices Act, 815 ILCS 505/1 *et seq.*, (hereinafter “ICFA”) prohibited “the use of any deception, fraud, false promise misrepresentation or concealment, suppression or omission of any material facts ... in the conduct of any trade of commerce” and declared such acts or practices unlawful.

74. Defendant’s acts and omissions alleged in this Complaint occurred in commerce.

75. Defendant represented to Plaintiff and Class Members that it had the capacity to protect Plaintiff’s PHI. This was false.

76. Defendant represented to Plaintiff and Class Members that it would comply with state and federal law regarding protection of Plaintiff’s and Class Members’ PHI. This was false.

77. Defendant represented to Plaintiff and Class Members that it would protect Plaintiff’s PHI. This was false.

78. Defendant violated the ICFA by the use of deceptive, false, and misleading misrepresentations or omissions of material fact in connection with securing Plaintiff’s PHI. In particular, Defendant lacked the capacity to protect Plaintiff’s PHI, Defendant failed to comply with applicable state and federal law regarding protection of Plaintiff’s and Class Members’ PHI, and Defendant failed to adequately protect Plaintiff’s and Class Members’ PHI.

79. Defendant intended that Plaintiff and Class Member would rely on its deceptive, false, and misleading misrepresentations or omissions of material fact when entrusting their PHI to Defendant.

80. As a direct and proximate result of Defendant’s violation of the ICFA, Plaintiff’s and Class Members’ PHI was entrusted to Defendant and was improperly accessed, copied, transferred, and/or disclosed.

81. As a direct and proximate result of Defendant’s violation of the ICFA, Plaintiff and Class Members have been harmed, damaged, and/or injured.

82. Defendants' conduct described in this claim for relief was outrageous because its acts showed a reckless disregard of the Plaintiff's and Class Members' rights.

COUNT V: NEGLIGENCE PER SE

83. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein, excluding Count I, II, III, and IV.

84. Defendant violated HIPAA by:

- a. Failing to ensure the confidentiality and integrity of electronic PHI Defendants created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);
- c. Failing to implement technical policies and procedures governing the receipt and removal of hardware and electronic media containing electronic PHI into and out of a facility to maintain security, in violation of 45 C.F.R. § 164.310(d)(1);
- d. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1);
- e. Failing to identify and respond to suspected or known security incidents or mitigate, to the extent practicable, harmful effects of security incidents that are known to Defendants, in violation of 45 C.F.R. § 164.308(a)(6)(ii);
- f. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. § 164.306(a)(2);
- g. Failing to protect against reasonably-anticipated impermissible uses or disclosures of

electronic PHI, in violation of 45 C.F.R. § 164.306(a)(3);

- h. Failing to ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(94);
- i. Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. § 164.502 *et seq.*;
- j. Failing to effectively train all members of their workforce (including independent contractors involved in the data breach) on the policies and procedures for PHI, as necessary and appropriate for the members of its workforce to carry out functions and maintain security of PHI, in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and
- k. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

85. Defendant agreed to ensure Agents complied with the same obligations as

Defendant with respect to the protection of Plaintiff's and Class Members' PHI.

86. Defendant's violation of HIPAA resulted in an injury to Plaintiff and Class Members.

87. Plaintiff and Class Members fall within the class of persons HIPAA was intended to protect.

88. The harms Defendant caused to Plaintiff and Class Members are injuries resulting from the type of behavior HIPAA was intended to prevent.

89. As a result, Plaintiff and Class Members have been harmed, damaged, and/or injured.

COUNT VI: BREACH OF COVENANT OF GOOD FAITH & FAIR DEALING

90. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein, excluding Counts I, II, III, IV, and V.

91. Every contract contains a covenant of good faith and fair dealing that prohibits a contracting party from intentionally depriving the other contracting party of the fruits of the contract (“Covenant”).

92. Through the conduct stated in this Complaint, Defendants breached the Covenant between Defendants and Plaintiff and Class Members.

93. Defendants agreed to ensure Agents complied with the same obligations as Defendants with respect to the protection of Plaintiff’s and Class Members’ PHI.

94. Defendant’s acts and omissions deprived Plaintiff and Class Members from receiving the fruits of the agreement.

95. Defendant’s breach of the Covenant proximately caused Plaintiff and Class Members to suffer harm and damages.

COUNT VII: INVASION OF PRIVACY

96. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein, excluding Counts I, II, III, IV, V, and VI.

97. Defendant’s misconduct, as described herein, and failure to encrypt, protect, secure, keep private, or otherwise keep Plaintiff’s and Class Members’ PHI constituted an invasion of Plaintiff’s and Class Members’ privacy.

98. Defendant agreed to ensure Agents complied with the same obligations as Defendant with respect to the protection of Plaintiff’s and Class Members’ PHI.

99. Said PHI is not a matter of public concern.

100. Defendant's failures, acts, omissions, and/or misconduct resulted in an unreasonable intrusion into the private lives and matters of Plaintiff and Class Members.

101. Defendant's failures, acts, omissions, and/or misconduct constituted a public disclosure of private facts, the nature of which a reasonable person of ordinary sensibilities would find objectionable and offensive.

102. As a direct result of Defendant's failures and misconduct, Plaintiff's and Class Members' PHI was disclosed to the public.

COUNT VIII: VICARIOUS LIABILITY

103. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein, excluding Counts I, II, III, IV, V, VI, and VII.

104. Defendant served as the employer and/or master of its employees, staff, or medical professionals.

105. Defendant has vicarious liability for the acts and omissions of all persons or entities under Defendant's control, either directly or indirectly, including its employees, agents, consultants, medical directors, and independent contractors, whether in-house or outside entities, individuals, or agencies causing or contributing to the injuries, damage, and harm to Plaintiff and Class Members.

106. Further, Defendant's employees, staff, agents, or medical professionals were in the line and scope of employment when they performed or failed to perform acts and/or omissions alleged herein.

107. Additionally, the acts and/or omissions Defendant's employees, staff, agents, or medical professionals performed or failed to perform were ratified by Defendant.

108. Defendant is vicariously liable for the acts of their employees, staff, agents, or medical professionals.

109. Such conduct was the proximate cause of Plaintiff's and Class Members' injury, damage, and harm.

COUNT IX: BAILMENT

110. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein, excluding Count I, II, III, IV, V, VI, VII, and VIII.

111. Plaintiff and Class Members delivered their personal and financial information to Defendant for the exclusive purpose of obtaining healthcare.

112. In delivering personal and financial information to Defendant, Plaintiff and Class Members intended and understood Defendant would adequately safeguard such information.

113. Defendant agreed to ensure Agents complied with the same obligations as Defendant with respect to the protection of Plaintiff's and Class Members' PHI.

114. Defendant accepted possession of Plaintiff's and Class Members' personal and financial information.

115. By accepting possession of Plaintiff's and Class Members' personal and financial information, Defendant understood Plaintiff and Class Members expected Defendant to adequately safeguard such personal and financial information, establishing a bailment (or deposit) for the mutual benefit of the parties.

116. During the bailment (or deposit), Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care, diligence, and prudence in protecting Plaintiff's and Class Members' personal and financial information.

117. Defendant breached this duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class Members' personal and financial information, resulting in the unlawful and unauthorized access to and misuse of Plaintiff's and Class Members' personal and

financial information.

118. Defendant further breached its duty to safeguard Plaintiff's and Class Members' personal and financial information by failing to timely and accurately notify Plaintiff and Class Members that their personal and financial information was compromised as a result of the data breach.

119. Defendant failed to return, purge, or delete Plaintiff's and Class Members' personal and financial information after the bailment (or deposit) and within the time limits allowed by law.

120. As a direct and proximate result of Defendant's breach of its duty, Plaintiff and Class Members suffered reasonably foreseeable consequential damages, including, but not limited to, the damages set forth above.

121. As a direct and proximate result of Defendant's breach of its duty, Plaintiff's and Class Members' personal and financial information entrusted to Defendant during the bailment (or deposit) was damaged and its value diminished.

RELIEF REQUESTED

Wherefore, Plaintiff, individually and on behalf of all other similarly situated, demands judgment in her favor and against Defendant as follows:

- a. Certify this case as a class action on behalf of the above-described Class Members and, if necessary, subclasses, and appoint Plaintiff as class representative and undersigned counsel as lead counsel;
- b. Find that Defendant is liable under all legal claims asserted herein for its failure to safeguard, secure, protect, keep private, and not disclose Plaintiff's and Class Members' PHI;

- c. Award injunctive and other equitable relief as necessary to protect the interests of the Class Members, including an Order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect all data collected through the course of its business in accordance with HIPAA and industry standards;
 - iii. requiring Defendant to provide lifetime consumer credit protection and monitoring services for Plaintiff and Class Members; and
 - iv. requiring Defendant to provide lifetime consumer credit insurance to provide coverage for unauthorized uses and disclosures of Plaintiff's and Class Members' personal information, medical information, and financial information;
- d. Award damages, including statutory damages where applicable and punitive damages, to Plaintiff and the Class Members in an amount to be determined at trial;
- e. Award restitution for any identity theft and misuse of identity, including, but not limited to, payment of any other costs, including attorneys' fees incurred by the victim in clearing the victim's credit history or credit rating, or any costs incurred in connection with any civil or administrative proceeding to satisfy any debt, lien, or other obligation of the victim arising as a result of Defendant's actions;
- f. Award restitution in an amount to be determined by an accounting of the differences between the price Plaintiff and Class Members paid in reliance upon Defendant's duty and promise to secure its members' PHI and the actual services - devoid of proper protection mechanisms - rendered by Defendant;

- g. Award Plaintiff and Class Members their reasonable litigation expenses and attorneys' fees;
- h. Award Plaintiff and Class members pre- and post-judgment interest to the maximum extent allowable by law; and
- i. Award such other and further legal and equitable relief as equity and justice may require.

Dated: September 16, 2020

Respectfully Submitted,

/s/ Troy Walton
WALTON TELKEN, LLC
Troy E. Walton
241 N. Main Street
Edwardsville, IL 62025
(618) 307-9880
twalton@waltontelken.com

&

TORHOERMAN LAW LLC
Kenneth J. Brennan
Tyler Schneider
210 South Main Street
Edwardsville, IL 62025
(618) 656-4400
k'brennan@thlawyer.com
tyler@thlawyer.com